UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JACK CARDWELL, individually and on behalf of all others similarly situated, Plaintiff, v. EMPRESS AMBULANCE SERVICE, LLC d/b/a EMPRESS EMERGENCY MEDICAL SERVICES f/k/a EMPRESS AMBULANCE SERVICE, INC., Defendant.	**Case No. _____** **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL DEMAND**

Plaintiff Jack Cardwell ("Plaintiff") brings this Class Action Complaint ("Complaint"), individually and on behalf of all others similarly situated, against Defendant Empress Ambulance Service, LLC d/b/a Empress Emergency Medical Services f/k/a Empress Ambulance Service, Inc. ("Empress EMS" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to Plaintiff, which are based on personal knowledge.

NATURE OF THE CASE

1. This class action arises from Defendant's failure to properly secure and safeguard the highly sensitive Electronic Protected Health Information of Plaintiff and Class Members, which included names, Social Security numbers, dates of service, and insurance information (collectively together, "e-PHI").

2. Plaintiff brings this class action for Defendant's failure to comply with industry and government regulatory standards to protect information systems that contain e-PHI and

Defendant's failure to provide adequate notice to Plaintiff and other Class Members that their e-PHI had been compromised.

3. Plaintiff seeks, among other things, damages and orders requiring Defendant to fully and accurately disclose the e-PHI and other information that has been compromised, to adopt reasonably sufficient security practices and safeguards to protect Plaintiff's and Class Members' e-PHI from unauthorized disclosures, and to prevent incidents like this unauthorized disclosure from occurring again in the future. Plaintiff further seeks an order requiring Defendant to provide identity theft protective services to Plaintiff and Class Members for ten (10) years, as Plaintiff and Class Members are at risk and will continue to be at an increased risk of identity theft due to the unauthorized disclosure of their e-PHI as a result of Defendant's conduct described herein.

4. Empress EMS is one of the New York's largest emergency and non-emergency response providers in Westchester, Rockland, Ulster, Dutchess, Putnam, Orange Counties, and the Bronx, including providing services with hospitals, correctional institutions, and private care facilities. Empress EMS "handles over fifty thousand transports a year."

5. Plaintiff received a notice letter from Empress EMS dated September 9, 2022 (the "Notice Letter"), indicating that on July 14, 2022, Empress EMS "identified a network incident resulting in the encryption of some of [their] systems" (the "Data Breach").

6. The Notice Letter went onto say that Empress EMS's "investigation determined that an unauthorized party first gained access to certain systems on our network on May 26, 2022, and then copied a *small subset of files* on July 13, 2022." (emphasis added).

7. The Notice Letter further stated that Empress EMS's "review identified documents containing [Plaintiff's] name, Social Security number, dates of service, and the name of your insurer, if on file with Empress EMS."

8. Under the Health Information Technology Act, healthcare organizations must report breaches affecting more than 500 people to the U.S. Department of Health and Human Services. On September 9, 2022, Empress EMS notified the U.S. Department of Health and Human Services Office for Civil Rights ("HHS OCR") that approximately 318,558 individuals were affected by the Data Breach.

9. However, contemporaneous news reporting by the technology industry website, *DataBreaches* have indicated that Empress EMS in its public statements dramatically underestimated the scope of the Data Breach, including that the Data Breach was a ransomware attack initiated by the "Hive" ransomware hacking group and that other categories of sensitive personally identifiable information were exfiltrated.

10. The Hive ransomware group started their ransomware attacks against organizations in June 2021 and quickly drew the attention of law enforcement due to a wide range of target industries, most notably healthcare. Hive ransomware uses the 'Ransomware-as-a-Service' model and double extortion method. If a victim fails to pay the ransom, Hive operators release the exfiltrated data on Hive's data leak sites on the dark web.

11. Correspondence from Hive to Empress shared exclusively with *DataBreaches* showed that Hive contacted Empress on July 14 and 15 by email. In their first email, Hive wrote, that it "[d]ownloaded most important information [sic] with a total size over 280 GB Few details about information we have downloaded: contracts, nda and other agreements documents; company private info (budgets, plans, investments, company bank statements, etc.); employees info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.); customers info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.);

SQL databases with reports, business data, customers data, etc.; approximate number of personal records including addresses and ssn's [sic] data is above 10000 units."

12. The Data Breach was a direct and proximate result of Defendant's flawed IT systems which was left susceptible to attack by cybercriminals.

13. Plaintiff's and Class Members' e-PHI, compromised by cybercriminals in the Data Breach, is highly valuable because it is readily useable to commit fraud and identity theft.

14. Such careless handling of e-PHI is prohibited by federal and state law. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires healthcare providers, like Defendant, and their business associates to safeguard patient e-PHI through a multifaceted approach that includes, among other things: (a) ensuring the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; (b) proactively identifying and protecting against reasonably anticipated threats to the security or integrity of e-PHI; (c) protecting against reasonably anticipated, impermissible uses or disclosures of e-PHI; (d) putting in place the required administrative, physical and technical safeguards to protect e-PHI; (e) implementing policies and procedures to prevent, detect, contain, and correct security violations; (f) effectively training their workforce regarding the proper handling of e-PHI; and (g) designating individual security and privacy officers to ensure compliance with these policies and procedures.

15. The type of e-PHI disclosed, including social security numbers, can be used to commit a host of fraud and identity theft, including but not limited to medical fraud, fraudulent unemployment claims, opening a new bank account, taking out a credit card, loan, or mortgage, and committing income tax refund fraud, as the IRS and several states require social security numbers to file a tax return. The cybercriminals who obtained Plaintiff's and Class Members' e-

PHI can use this information to commit the aforementioned crimes and can sell this information to other identity thieves who will do the same.

16. Consequently, Plaintiff and Class Members have devoted significant time to protecting themselves as a result of Defendant's actions and Plaintiff and Class Members will need to spend additional time and money in the future to that same end.

17. Plaintiff, individually and all others similarly situated, brings claims for negligence, negligence *per se*, breach of implied contract, New York General Business Law § 349, and injunctive relief claims.

18. Plaintiff seeks damages and injunctive relief requiring Defendant to adopt reasonably sufficient practices to safeguard the e-PHI that remains in Defendant's custody in order to prevent incidents like the Data Breach from reoccurring in the future. Given that information relating to the Data Breach, including the systems that were impacted, Plaintiff anticipates additional support for his claims will be uncovered following a reasonable opportunity for discovery.

PARTIES

A. Plaintiff

19. Plaintiff Jack Cardwell ("Plaintiff") is a resident of Westchester County, New York.

20. On or around on June 9, 2018, Empress EMS treated and transported Plaintiff to the hospital.

21. Plaintiff received the Notice Letter from Empress EMS dated September 9, 2022, indicating that his e-PHI was compromised as part of the Data Breach.

22. Plaintiff's e-PHI was disclosed without his authorization to unknown third parties as a result of Defendant's Data Breach.

23. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time and resources in an effort to detect and prevent any additional misuses of his e-PHI. Plaintiff would not have to undergo such costly and time-consuming efforts but for the Data Breach.

24. Since the Data Breach, Plaintiff has each already spent significant time on the phone and internet monitoring their accounts, dealing with the credit agencies and the IRS, and attempting to learn about the full extent of the Data Breach. Plaintiff estimates he spent approximately two hours on these efforts.

25. Plaintiff would not have given his e-PHI to Defendant if he had known that Defendant were going to maintain his e-PHI without adequate security protection.

26. As a result of the Data Breach, Plaintiff has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the e-PHI compromised by the Data Breach.

B. Defendant

27. Defendant Empress Ambulance Service, LLC d/b/a Empress Emergency Medical Services f/k/a Empress Ambulance Service, Inc. ("Empress EMS" or "Defendant") is a Delaware limited liability company with its principal place of business located in Yonkers, New York. In July 2019 Empress Ambulance Service, Inc. was purchased by Paramedics Logistics Operating Company, LLC and converted into Empress Ambulance Service, LLC.

28. Empress EMS is an emergency and non-emergency response provider in Westchester, Rockland, Ulster, Dutchess, Putnam, Orange Counties, and the Bronx, including with hospitals, correctional institutions, and private care facilities.

JURISDICTION AND VENUE

29. The Court has subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) because Plaintiff and Defendant are citizens of different states and the amount in controversy exceeds $5,000,000.

30. The Court also has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367(a) because the state law claims are related to claims in the action within such original jurisdiction and they form part of the same case or controversy under Article III of the United States Constitution.

31. This Court has personal jurisdiction over Empress EMS because (1) Empress EMS conducts a substantial business in and throughout New York, where there are a considerable number of patients; (2) Empress EMS's headquarters are located in New York; and (3) the wrongful acts alleged in the Complaint caused harm to Plaintiff and Class Members in New York.

32. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b)(2), because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

33. In Empress EMS's September 9, 2022 Notice Letter to Plaintiff and Class Members, Empress EMS stated publicly for the first time that on July 14, 2022, Empress EMS "identified a network incident resulting in the encryption of some of [their] systems." Empress EMS's "investigation determined that an unauthorized party first gained access to certain systems on [their] network on May 26, 2022, and then copied a small subset of files on July 13, 2022."

34. According to Empress EMS's Notice Letter the "small subset of files" included names, Social Security number, dates of service, and the name of a patient's insurer if on file with Empress EMS.

35. On September 9, 2022, Empress EMS also notified HHS OCR that approximately 318,558 individuals were affected by the Data Breach.

36. However, it appears that Empress EMS's public statements dramatically underestimated the scope of the Data Breach, including that the Data Breach was a ransomware attack initiated by the Hive ransomware hacking group and that other sensitive personally identifiable information, including employee social security numbers as well as patients' passports was exfiltrated.

37. According to correspondence from Hive to Empress EMS, shared exclusively with the technology industry website, *DataBreaches*, showed that Hive contacted Empress EMS on July 14 and 15 by email. As described in Figure-1 below, in their first email, Hive wrote, in part:

FIGURE-1

! ! ! DO NOT TRY TO DECRYPT OR CHANGE ENCRYPTED FILES ON YOUR COMPUTERS, IT WILL COMPLETELY DESTROY THEM ! ! !

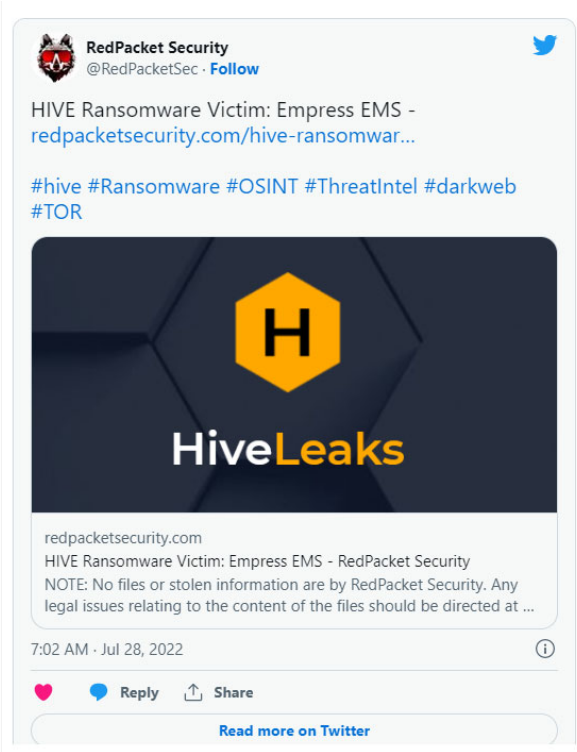
Ladies and gentlemen! Attention, please!
This is HIVE ransomware team.

We infiltrated your network and stayed there for 12 days (it was enough to study all your documentation and gain access to your files and services),
encrypted your servers.
Downloaded most important information with a total size over 280 GB
Few details about information we have downloaded:
– contracts, nda and other agreements documents
– company private info (budgets, plans, investments, company bank statements, etc.)
– employees info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.)
– customers info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.)
– SQL databases with reports, business data, customers data, etc.
– approximate number of personal records including addresses and ssn's data is above 10000 units

38. A sample of files provided to Empress EMS with Hive's July 15 email, also provided to *DataBreaches*, included protected health information of some of Empress EMS's patients. Hive claimed to have more than 100,000 Social Security numbers as part of the data they exfiltrated.

39. According to *DataBreaches*, Empress EMS's exfiltrated data set briefly appeared on the dark web in July 2022—long enough to be detected by *RedPacket Security* who tweeted a link containing the dark web domain name address for the public to access. *See* Figure-2 below:

FIGURE-2



40. e-PHI pertaining to Plaintiff was part of the data acquired by unauthorized third parties from Empress EMS's systems in the Data Breach.

41. The Notice Letter states that Empress EMS "conducted a thorough investigation with the assistance of a third-party forensic firm." Additional items of e-PHI as well as other facts

surrounding the Data Breach may be uncovered or have already been uncovered and not yet publicly disclosed.

42. The Notice Letter states that since discovering the Data Breach, Empress EMS is "implementing new network security measures and providing additional training to our employees to help prevent something like this from happening in the future." Empress EMS also posted a "Notice of Security Incident" on its website where it states: "to help prevent something like this from happening again, we strengthened the security of our systems and will continue enhancing our protocols to further safeguard the information in our care." These are steps that should have been employed in the first place-and which would have prevented or limited the impact of the Data Breach.

43. Discovery of Defendant, "law enforcement," and Empress EMS's "third-party forensic firm" will reveal more specific facts about Defendant's deficient and unreasonable security procedures.

44. The Notice Letter states that affected customers should obtain credit monitoring and identity theft protection services to help them detect possible misuse of e-PHI, which Empress is providing for only one year.

45. As a result of the Data Breach, Plaintiff and Class Members have been and must continue to be vigilant and review their credit reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

B. Data Security Industry Standards

46. Defendant is well aware of the importance of safeguarding Plaintiff's and Class Members' e-PHI, that by virtue of their business—emergency medical services—they place Plaintiff's and Class Members' e-PHI at risk of being targeted by cybercriminals.

47. Defendant is aware that the e-PHI that they collect, organize, and store, can be used by cybercriminals to engage in crimes such as identity fraud and theft using Plaintiff's and Class Members' e-PHI.

48. Because Defendant failed to implement, maintain, and comply with necessary cybersecurity requirements, as a result, Defendant was unable to protect Plaintiff's and Class Members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality.

49. As a proximate result of such failures, cybercriminals gained unauthorized access to Defendant's network unimpeded and acquired Plaintiff's and Class Members' e-PHI in the Data Breach without being stopped.

50. Only after discovering the Data Breach did Defendant begin to undertake basic steps recognized in the industry to protect Plaintiff's and Class Members' e-PHI.

51. Defendant was unable to prevent the Data Breach and was unable to detect the unauthorized access to vast quantities of sensitive and protected files containing Plaintiff's and Class Members' e-PHI.

52. Commonly accepted data security standards among businesses that store personal and financial information, such as the e-PHI involved here, include, but are not limited to:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for personal and financial information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

53. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for Cybersecurity (*Start with Security: A Guide for Business*, (June 2015)) and protection of personal and financial information (*Protecting Personal Information: A Guide for Business*, (Oct. 2016)), which includes basic security standards applicable to all types of businesses.

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. Because Defendant was entrusted with Plaintiff's and Class Members' e-PHI, they had and have a duty to keep the e-PHI secure.

56. Plaintiff and Class Members reasonably expect that when they provide their e-PHI to Empress EMS they will safeguard their information.

57. Despite Defendant's obligations, Defendant failed to appropriately monitor and maintain their data security systems in a meaningful way so as to prevent the Data Breach.

58. Had Defendant properly maintained their systems and adequately protected them, they could have prevented the Data Breach.

C. The Value of e-PHI

59. e-PHI, including the information involved here, can be used for malicious purposes, including financial fraud, medical identity theft, identity theft, insurance fraud, and crafting convincing phishing messages. The U.S. Department of Health and Human Services has listed a number of scenarios that exploit patient data:

a. *medical identity theft*—the use of another person's medical information to obtain a medical service;

b. *weaponizing of medical data*—the use of sensitive medical data to threaten, extort, or influence individuals;

c. *financial fraud*—the use of personally identifiable information contained in medical records to create credit card or bank profiles to facilitate financial fraud; and

d. *cyber campaigns*—the use of medical data as complementary data in future hacking campaigns.

60. As a result, e-PHI has become increasingly valuable on the black market. For example, according to Forbes, as of April 14, 2017, the going rate for an SSN is $0.10 cents and a credit card number is worth $0.25 cents, but medical records containing e-PHI could be worth hundreds or even thousands of dollars. For example, in April of 2019, HHS estimated that the average price of medical records containing e-PHI ranged between $250 and $1,000.

61. According to The World Privacy Forum, a nonprofit public interest group, one of the reasons for this price differential is that criminals are able to extract larger illicit profits using

medical records than they are for a credit card or SSN. For example, while a credit card or SSN typically yields around $2,000 before being canceled or changed, an individual's e-PHI typically yields $20,000 or more. This is because, in addition to the fact that healthcare data and e-PHI are immutable (*e.g.*, you cannot cancel your medical records), healthcare data breaches often take much longer to be discovered, allowing thieves to leverage e-PHI for an extended period of time.

62. Researchers at HealthITSecurity.com have also reported criminals selling illicit access to compromised healthcare systems on the black market, which would give other criminals "access to their own post-exploitation activity, such as obtaining and exfiltrating sensitive information, infecting other devices in the compromised network, or using connections and information in the compromised network to exploit trusted relationships between the targeted organizations and other entities to compromise additional networks."

D. Defendant Failed to Comply with HIPAA, the National Standard for Protecting Private Health Information

63. HIPAA requires the healthcare industry to have a generally accepted set of security standards for protecting health information. HIPAA defines Protected Health Information ("PHI") as individually identifiable health information and e-PHI that is transmitted by electronic media or maintained in electronic media. This protected information includes: names, dates, phone numbers, fax numbers, email addresses, *Social Security numbers*, medical record numbers, health insurance beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, photographs, and any other unique identifying number, characteristic, or code.

64. To this end, HHS promulgated the *HIPAA Privacy Rule* in 2000 and the *HIPAA Security Rule* in 2003. The security standards for the protection of e-PHI, known as "the Security

Rule," establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities," must put in place to secure individuals' e-PHI.

65. Defendant is either an entity covered by HIPAA, *see* 45 C.F.R. § 160.102, or "business associates" covered by HIPAA, *see* 45 C.F.R. § 160.103, and therefore must comply with the HIPAA Privacy Rule and Security Rule, *see* 45 C.F.R. Part 160 and Part 164, Subpart A, C, and E.

66. HIPAA limits the permissible uses of e-PHI and prohibits the unauthorized disclosure of e-PHI. *See* 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

67. The electronically stored images and healthcare information accessed by unauthorized third parties on Defendant's servers are e-PHI under the HIPAA Privacy Rule and the Security Rule, which protects all e-PHI a covered entity "creates, receives, maintains or transmits" in electronic form. 45 C.F.R. § 160.103.

68. The Security Rule requires covered entities, including Defendant to implement and maintain appropriate administrative, technical, and physical safeguards for protecting e-PHI. *See* 45 C.F.R. § 164.530(c)(1). Among other things, the Security Rule requires Empress EMS to identify and "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of [the] information" and "[p]rotect against any reasonably anticipated uses or disclosures." 45 C.F.R. § 164.306.

69. HIPAA also obligates Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations. *See* 45 C.F.R. § 164.308(a)(1)(i).

70. HIPAA further obligates Defendant to ensure that their workforces comply with HIPAA security standard rules, *see* 45 C.F.R. § 164.306(a)(4), to effectively train their workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

71. Defendant failed to comply with these HIPAA rules. Specifically, Empress EMS failed to put in place the necessary technical and non-technical safeguards required to protect Plaintiff's and other Class members' e-PHI.

E. Defendant Violated Their Common Law Duty of Reasonable Care

72. Defendant was aware of the importance of security in maintaining personal information (particularly sensitive personal and financial information like the e-PHI involved here), and the value consumers place on keeping their e-PHI secure.

73. In addition to obligations imposed by federal and state law, Defendant owed and continues to owe a common law duty to Plaintiff and Class Members—who entrusted Defendant with their e-PHI—to exercise reasonable care in receiving, maintaining, and storing, the e-PHI in Defendant's possession.

74. Defendant owed and continue to owe a duty to prevent Plaintiff's and Class Members' e-PHI from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Defendant's duty was (and is) the obligation to provide reasonable security consistent with current industry best practices and requirements, and to ensure information technology systems and networks, in addition to the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiff's and Class Members' e-PHI.

75. Defendant owed a duty to Plaintiff and Class Members, who entrusted Defendant with extremely sensitive e-PHI to design, maintain, and test the information technology systems that housed Plaintiff's and Class Members' e-PHI, to ensure that the e-PHI in Defendant's possession was adequately secured and protected.

76. Defendant owed a duty to Plaintiff and Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the e-PHI stored in Defendant's systems. In addition, this duty also required Empress EMS to adequately train its employees and others with access to Plaintiff's and Class Members' e-PHI on the procedures and practices necessary to safeguard such sensitive information. This duty also required supervision, training, and compliance on Empress's part to ensure that it complied with creating, implementing, and maintaining reasonable data security practices and procedures sufficient to protect Plaintiff's and Class Members' e-PHI.

77. Defendant owed a duty to Plaintiff and Class Members to implement processes that would enable Defendant to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

78. Defendant owed a duty to Plaintiff and Class Members to disclose when and if their information technology systems and data security practices were not sufficiently adequate to protect and safeguard Plaintiff's and Class Members' e-PHI.

79. Defendant violated these duties. The Notice Letter further states that Empress EMS became aware of it on July 14, 2022, however Plaintiff and Class Members, and the public did not learn of the Data Breach until September 9, 2022, when the Notice Letters were mailed out. Defendant failed to publicly describe the full extent of the Data Breach and notify affected parties.

This demonstrates that Empress EMS did not properly implement measures designed to timely detect a data breach of their information technology systems, as required to adequately safeguard Plaintiff's and Class Members' e-PHI.

80. Defendant also violated their duty to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiff's and Class Members' e-PHI.

81. As the Notice Letter states, Empress EMS "took measures to contain the incident, reported it to law enforcement, and we conducted a thorough investigation with the assistance of a third-party forensic firm." Empress EMS could have taken these steps *beforehand* to protect the e-PHI in their possession and prevent the Data Breach from occurring, as required under FTC guidelines and HIPAA, as well as other state and federal law and/or regulations.

82. Thus, Defendant owed a duty to Plaintiff and Class Members to timely disclose the fact that a data breach, resulting in unauthorized access to their e-PHI, had occurred.

F. The Value of Private Information and Effects of Unauthorized Disclosure

83. Defendant was well aware that the protected e-PHI it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the e-PHI and those who would use it for wrongful purposes.

84. e-PHI is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld.

85. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

86. The forms of e-PHI involved in this Data Breach are particularly concerning, including:

87. ***Social security numbers***—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

88. Indeed, even the Social Security Administration warns that the process of replacing a social security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.

> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

89. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of e-PHI to steal and then sell.

90. ***Insurance information***—stolen insurance information, such as the e-PHI that was involved here—*name of insurer*—can also result in cybercriminals taking out fraudulent insurance policies or submitting fraudulent insurance claims in a person's name

91. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' e-PHI secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

92. Thus, Defendant knew, or should have known, the importance of safeguarding the e-PHI entrusted to it and of the foreseeable consequences if its systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

93. As highly sophisticated parties that handle sensitive e-PHI, Defendant failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to

ensure the security and confidentiality of Plaintiff's and other Class Members' e-PHI to protect against anticipated threats of intrusion of such information.

94. Identity thieves use stolen e-PHI for various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud and government fraud.

95. The e-PHI exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

96. There is often a lag time between when fraud occurs versus when it is discovered, as well as between when e-PHI is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

97. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

98. Plaintiff and Class Members rightfully place a high value not only on their e-PHI, but also on the privacy of that data.

99. Thus, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

100. Data breaches are preventable. As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…" and "[m]ost of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures…Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

101. Here Empress EMS after the Data Breach "took measures to contain the incident," "are implementing new network security measures and providing additional training to our employees to help prevent something like this from happening in the future," but should have implemented them in advance to prevent the Data Breach.

102. The types e-PHI, such as Social Security numbers, compromised in the Data Breach are immutable. Plaintiff and Class Members are not able to change them or simply cancel them, like a credit card, to avoid harm or fraudulent use of the information. Just like a birthdate or a mother's maiden name, these pieces of information cannot be changed by logging into a website and changing them in settings, and they can be used alone or in conjunction with other pieces of Plaintiff's and Class Members' information to commit serious identity theft and fraud.

G. Defendant Obtains, Collects, and Stores Plaintiff's and Class Members' e-PHI

103. In the ordinary course of doing business as an ambulatory service provider, Empress EMS requires its patients to provide their sensitive e-PHI in order to obtain treatment and transport.

104. The Notice Letter indicates that names, Social Security numbers, dates of service, and name of insurer were acquired by cybercriminals, yet this appears to conflict with the broader data set *DataBreaches* reported that the Hive ransomware group was able to exfiltrate. *See* Figure-1, *supra*. The logical inference is that additional information regarding the Data Breach is yet to be uncovered, which may reveal additional misconduct or other fields of valuable information not already specified.

105. By obtaining, using, disclosing, and deriving a benefit from Plaintiff's and Class Members' e-PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' e-PHI from unauthorized disclosure.

106. Thus, Defendant had access to Plaintiff's and Class Members' e-PHI which was stored on their systems.

107. Plaintiff and Class Members reasonably expected that their ambulatory service provider would use the utmost care to keep their e-PHI confidential and securely maintained.

108. Empress EMS acknowledges in its Notice Letter to Plaintiff and Class Members its obligation to protect and secure e-PHI: "we are committed to protecting the privacy and security of our patients' information," and "[w]e value the trust our community places in Empress EMS."

109. Despite Defendant's obligation to protecting personal information, Defendant failed to prioritize data and cybersecurity by adopting reasonable data and cybersecurity measures to prevent and detect the unauthorized access to Plaintiff's and Class Members' e-PHI.

110. Had Defendant remedied the security deficiencies, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented intrusion into its information systems and, ultimately, the theft of Plaintiff's and Class Members' e-PHI.

H. Defendant Failed to Comply with the FTC Act

111. Defendant are prohibited by the FTC Act, 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

112. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates the FTC Act.

113. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

114. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The

guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

115. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

116. Defendant is aware of and failed to follow the FTC guidelines and failed to adequately secure e-PHI.

117. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

118. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer e-PHI, or to prevent the disclosure of such information to unauthorized individuals constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

119. Defendant were at all times fully aware of their obligations to protect the e-PHI of consumers because of its business of obtaining, collecting, and storing e-PHI. Defendant were also aware of the significant repercussions that would result from their failure to do so.

I. Defendant Violated Their Own Privacy Policies

120. Plaintiff and Class Members entrusted Defendant with an extensive amount of their sensitive e-PHI. Defendant understands the importance of protecting such information.

121. Empress EMS has dedicated a section on its website to apprise its customers and patients, including Plaintiff and Class members, of the permissible uses and disclosure of their e-PHI. More specifically, Empress EMS posts on its website, the Notice of Privacy Practices ("Privacy Practices").

122. Empress EMS's Privacy Practices states: "Empress Ambulance Service, Inc. is committed to protecting your personal health information. We are required by law to maintain the privacy of health information that could reasonably be used to identify you, known as 'protected health information' or 'PHI'…We respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times."

123. The Privacy Practices lists the permitted uses and disclosures of patients' e-PHI that Empress EMS can make without patient authorization, including: treatment; healthcare operations; fundraising; reminders for scheduled transports and information on other services; to another healthcare provider; for healthcare fraud and abuse detection or for activities related to compliance with the law; to a family member if consent is obtained; to a public health authority in certain situations; for health oversight activities including audits; for judicial and administrative proceedings, as required by a court or administrative order; for law enforcement activities in limited situations; for military, national defense and security and other special government functions; to avert a serious threat to the health and safety of a person or the public at large; for workers' compensation purposes; to coroners, medical examiners, and funeral directors; if an

organ donor to organizations that handle organ procurement or transplantation; for research projects, subject to strict oversight and approvals.

124. For all other situations—*i.e.*, those not covered by routine or compelled disclosure above—Empress EMS's Privacy Practices explicitly promised that: "[a]ny other use or disclosure of PHI, other than those listed above, will only be made with your written authorization (the authorization must specifically identify the information we seek to use or disclose, as well as when and how we seek to use or disclose it)." Plaintiff provided no such authorization.

125. By these representations in the Privacy Practices, Defendant has affirmatively—and misleadingly—assured patients, including Plaintiff and the Class Members, that they had the ability to control the dissemination of their e-PHI and to restrict its use and access by third parties. The Privacy Practices also expressly guaranteed Defendant would safeguard Plaintiff's and Class Member's e-PHI consistent with the applicable laws and regulations ("We are required by law to maintain the privacy of health information that could reasonably be used to identify you, known as 'protected health information" or 'PHI.'").

126. However, Defendant failed to safeguard patients' e-PHI in violation of their own Privacy Practices and applicable law and regulations, as confirmed by Defendant's own admission in their September 9, 2022 Notice Letter, in which Defendant admit that: "*an unauthorized party* first gained access to certain systems on our network" (emphasis added). In fact, Defendant failed to take *any* steps to safeguard Plaintiff's and Class Members' e-PHI until after the Data Breach occurred.

127. Defendant's failure to implement appropriate security measures and adequately safeguard Plaintiff's and Class Members' e-PHI violated the terms of their own Privacy Practices.

128. Despite these promises and assurances to protect its customers' e-PHI, Empress EMS failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized third-party access to Plaintiff's and Class Members' e-PHI.

129. Defendant's failure to implement appropriate security measures and adequately safeguard Plaintiff's and Class Members' e-PHI violated the terms of their own policies.

J. Plaintiff and Class Members Suffered Damages

130. The ramifications of Defendant's failure to keep e-PHI secure are long-lasting and severe. Victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.

131. Plaintiff and Class Members have faced a substantial and imminent risk of identity theft and fraud as a result of the Data Breach. Unauthorized third parties carried out the Data Breach and stole the personal information of Plaintiff and Class Members with the intent to use it for fraudulent purposes and/or sell it to other cybercriminals.

132. The risk of identity theft is particularly substantial when the e-PHI compromised is unique to a specific individual, as it is here, and is extremely sensitive Social Security numbers.

133. Plaintiff and Class Members will spend substantial amounts of their money and time monitoring their accounts for identity theft and fraud and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming.

134. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their e-PHI.

135. Besides damage sustained in the event of identity theft, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues. The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

136. Despite all of the publicly available knowledge of the continued compromises of e-PHI and the importance of securing such information, Defendant's commitment to secure its customers' information fell by the wayside.

137. Empress EMS was well aware of the requirements and obligations to secure e-PHI. Further, Empress EMS had control over the configuration and design of its own systems, and knowingly chose to forego the necessary data protection techniques needed for it to secure Plaintiff's and Class Members' e-PHI.

138. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable e-PHI; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their e-PHI being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their e-PHI; and continued risk to Plaintiff's and the Class Members' e-PHI, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect the e-PHI that was entrusted to it.

CLASS ALLEGATIONS

139. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following nationwide class:

> All persons residing in the United States whose e-PHI was accessed, acquired, used, or disclosed as a result of the Data Breach Defendant revealed on September 9, 2022 ("the Class").

140. Excluded from the Class are Defendant, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendant have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

141. Plaintiff reserves the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

142. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. Empress EMS's disclosure to HHS OCR indicates that approximately 318,558 individuals were affected by the Data Breach.

143. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the information implicated in the Data Breach.

144. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class Members. The questions

of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant had a duty to secure and protect the e-PHI of Plaintiff and Class Members;

b. Whether Defendant were negligent in collecting and disclosing Plaintiff's and Class Members' e-PHI;

c. Whether Defendant had duties not to disclose the e-PHI of Plaintiff and Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' e-PHI;

e. Whether Defendant failed to adequately safeguard the e-PHI of Plaintiff and Class Members;

f. Whether Defendant breached their duties to exercise reasonable care in handling Plaintiff's and Class Members' e-PHI in the manner alleged herein, including failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant had respective duties not to use the e-PHI of Plaintiff and Class Members for non-business purposes;

i. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their e-PHI had been compromised;

j. Whether Plaintiff and Class Members are entitled to declaratory judgment under 28 U.S.C. § 2201, *et seq.*;

k. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

145. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of Class Members. The claims of the Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard e-PHI. Plaintiff and Class Members each had their e-PHI disclosed by Defendant to an unauthorized third party.

146. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class Members. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation, including data breach litigation. The claims of Plaintiff and Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the Class Members are likely to be substantial, the damages suffered by the individual Class Members are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while

protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

147. Here a class action is superior to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go un-remedied.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

148. Plaintiff restates and reallege all proceeding allegations above as if fully set forth herein.

149. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their e-PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

150. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendant's systems to ensure that Plaintiff's and Class Members' e-PHI in Defendant's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own security systems, regarding intrusions to its

networks; (d) maintaining data security measures consistent with industry and governmental regulator standards.

151. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

152. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable e-PHI that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

153. Defendant had a duty not to engage in conduct that creates a foreseeable risk of harm to Plaintiff and Class Members.

154. Defendant breached the duties owed to Plaintiff and Class Members and thus were negligent. Specifically, Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the e-PHI of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry and governmental regulator standards; and (d) disclose that Plaintiff's and Class Members' e-PHI in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

155. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their e-PHI would not have been compromised.

156. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

(a) Theft of their e-PHI;

(b) Costs associated with requested credit freezes;

(c) Costs associated with the detection and prevention of identity theft;

(d) Costs associated with purchasing credit monitoring and identity theft protection services;

(e) Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of Defendant's Data Breach;

(f) The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their e-PHI being disclosed to cybercriminals;

(g) Damages to and diminution in value of their e-PHI entrusted, directly or indirectly, to Defendant with the societal understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; and

(h) Continued risk of exposure to hackers and thieves of their e-PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members.

157. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

158. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years.

COUNT II
NEGLIGENCE *PER SE*

159. Plaintiff restates and reallege all proceeding allegations above as if fully set forth herein.

Negligence *Per Se* Under Section 5 of the FTC Act

160. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to use reasonable measures to protect e-PHI. Various FTC publications and orders also form the basis of Defendant's duty.

161. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect e-PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of e-PHI it obtained and disclosed and the foreseeable consequences of a data breach.

162. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

163. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

164. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

165. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

166. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years.

Negligence *Per Se* Under HIPAA

167. The HIPAA Security Rule requires Defendant to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI, which Defendant negligently failed to implement. The HIPAA Security Rule requires Defendant to protect against reasonably anticipated threats to the security or integrity of e-PHI and protect against reasonably anticipated impermissible uses or disclosures, which Defendant negligently failed to do. *See* 45 C.F.R. Part 160 and Part 164, Subpart A, C, and E.

168. Plaintiff and Class Members, as patients of Empress EMS, are within the class of persons the HIPAA Security Rule was intended to protect. The harm that has occurred is the type of harm the HIPAA Security Rule was intended to guard against.

169. Defendant's failure to secure Plaintiff's and Class Members' e-PHI and to notify them that such information had been accessed by unauthorized third parties violated at least the following HIPAA regulations:

A) The HIPAA Privacy and Security Rule 45 C.F.R. § 160 and 45 C.F.R. § 164, Subpart A, C, and E

- 45 C.F.R. § 164.306
- 45 C.F.R. § 164.308
- 45 C.F.R. § 164.312
- 45 C.F.R. § 164.314

- 45 C.F.R. § 164.502
- 45 C.F.R. § 164.530

170. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

171. Defendant's violation of the HIPAA Privacy and Security Rule constitutes negligence *per se*.

172. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years.

183 Whether under Section 5 of the FTC Act or under HIPAA, each independently constitutes negligence *per se*.

COUNT III
BREACH OF IMPLIED CONTRACT

184 Plaintiff restates and reallege all proceeding allegations above as if fully set forth herein.

185 When Defendant required Plaintiff and Class Members to supply their e-PHI, Defendant entered into implied contracts with Plaintiff and Class Members to protect the security of such information.

186 Defendant collects and uses Plaintiff's and Class Member's e-PHI for the purpose of treating and transporting patients who need ambulatory services.

187 Such implied contracts arose from the course of conduct between Plaintiff and Class Members and Defendant.

188 The implied contracts required Defendant to safeguard and protect Plaintiff's and Class Members' e-PHI from being compromised and/or stolen.

189 Defendant did not safeguard or protect Plaintiff's and Class Members' e-PHI from being accessed, compromised, and/or stolen. Defendant did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiff's and Class Members' e-PHI.

190 Because Defendant failed to safeguard and/or protect Plaintiff's and Class Members' e-PHI from being compromised or stolen, Defendant breached its contracts with Plaintiff and Class Members.

191 Plaintiff and Class Members fully performed their obligations under the implied contracts by supplying their e-PHI to Defendant and paying Defendant for their services.

192 As a direct and proximate result of Defendant's breaches of implied contracts, Plaintiff and Class Members sustained damages as alleged herein and will continue to suffer damages as the result of Defendant's Data Breach.

193 Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

194 Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years.

COUNT IV
VIOLATION OF NEW YORK GEN. BUS. LAW § 349, *et seq.*

195 Plaintiff restates and reallege all proceeding allegations above as if fully set forth herein.

196 As a consumer of Empress EMS's services, Plaintiff is authorized to bring a private action under New York's Uniform Deceptive Trade Practices Act, Gen. Bus. Law § 349(h) ("GBL § 349(h)").

197 Plaintiff is a "person" within the meaning of GBL § 349.

198 Plaintiff and Class Members provided their e-PHI to Empress EMS pursuant to transactions in "business" "trade" or "commerce" as meant by GBL § 349.

199 The GBL prohibits "deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state." GBL § 349(a).

200 This Count is brought for Defendant's deceptive conduct, including their unlawful and deceptive acts related to the breach alleged herein.

201 Defendant engaged in unlawful and deceptive acts and practices in the conduct of trade or commerce and furnishing of services purchased by Plaintiff and the Class in violation of GBL § 349, including but not limited to the following:

a. Defendant failed to implement adequate privacy and security measures to protect Plaintiff's and Class Members' e-PHI from being accessed, acquired, used, or disclosed by unauthorized third parties, which was a direct and proximate cause of Plaintiff's and Class Members' harm;

b. Defendant's representation that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' e-PHI from being accessed, acquired, used, or disclosed by unauthorized third parties was unfair and deceptive given the inadequacy of its privacy and security protections;

c. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for Plaintiff's and Class Members' e-PHI;

d. Defendant's negligence in failing to disclose the material fact of its inadequate privacy and security protections for Plaintiff and Class Members e-PHI was deceptive in light of representations that they would comply with, among other things, HIPAA;

e. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff's and Class Members' e-PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in Plaintiff's and the Class's e-PHI being accessed, acquired, used, or disclosed by unauthorized third parties. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA; and

202 The above unfair and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

203 Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' e-PHI and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing, and reckless with respect to the rights of Plaintiff and Class Members.

204 Plaintiff and Class Members relied on Defendant's deceptive acts and practices when they paid money in exchange for goods and services and provided their e-PHI to Empress EMS for treatment and transport.

205 Plaintiff and Class Members relied on Defendant to safeguard and protect their e-PHI and to timely and accurately notify them if their data had been accessed by unauthorized third parties.

206 Plaintiff and Class Members seek all available relief under the New York GBL § 349 *et seq*.

COUNT V
DECLARATORY JUDGMENT

207 Plaintiff restates and reallege all proceeding allegations above as if fully set forth herein.

208 Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

209 An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' e-PHI and whether Defendant are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their e-PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his e-PHI and remain at imminent risk that further compromises of their e-PHI will occur in the future. It is unknown what "new network security measures" and "additional training to our employees" that Defendant has "implemented" and "provided" in response to the Data Breach.

210 Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure consumers' e-PHI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, HIPAA, N.Y. GBL § 349, *et seq.*;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' e-PHI; and

c. Defendant's ongoing breaches of its legal duty continues to cause Plaintiff harm.

211 This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect Plaintiff's and Class Members' e-PHI. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards;

d. implement an education and training program for appropriate employees regarding cybersecurity.

212 If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not

have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

213 The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

214 Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and all others similarly situated, prays for relief as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(c) For damages in an amount to be determined by the trier of fact;

(d) For an order of restitution and all other forms of equitable monetary relief;

(e) Declaratory and injunctive relief as described herein;

(f) Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

(g) Awarding pre- and post-judgment interest on any amounts awarded; and

(h) Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: October 10, 2022

Respectfully submitted

/s/ Christian Levis

Christian Levis
Amanda G. Fiorilla
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Email: clevis@lowey.com
Email: afiorilla@lowey.com

Anthony M. Christina (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Email: achristina@lowey.com

Counsel for Plaintiff and the Proposed Class